

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number: 10559-0754001 / P13652
	Application Number 10/066,070	Filed February 1, 2002
	First Named Inventor Satyendra Yadav	
	Art Unit 2435	Examiner Leynna Thanh Truvan

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

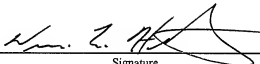
I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record 47,671
(Reg. No.)

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____



Signature
William E. Hunter

Typed or printed name
(858) 678-5070

Telephone number
March 9, 2009

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Satyendra Yadav	Art Unit :	2435
Serial No. :	10/066,070	Examiner :	Leynna Thanh Truvan
Filed :	February 1, 2002	Conf. No. :	2485
Title :	APPLICATION-SPECIFIC NETWORK INTRUSION DETECTION		

MAIL STOP AF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Pursuant to the Pre-Appeal Brief Conference Program, a request for a review of identified matters on appeal is hereby submitted in view of clear legal or factual deficiencies in the rejections. All rights to address additional matters in the full appeal brief are hereby reserved.

Claims 21-28 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Kouznetsov (U.S. Patent 6,973,577), and further in view of Gryaznov (U.S. Patent 7,065,790). Independent claim 21 recites, in part, “one or more machines coupled with the network, each machine comprising a communication interface and a memory including an execution area configured to perform operations comprising examining a set of instructions embodying an invoked application to identify the invoked application, obtaining application-specific intrusion criteria, and monitoring network communications for the invoked application, after the examining and the obtaining, using the application-specific intrusion criteria to detect an intrusion.” Kouznetsov fails to teach or suggest the claimed subject matter, either alone or in combination with Gryaznov.

Kouznetsov teaches a system and a method for dynamically detecting computer viruses through associative behavioral analysis of runtime state.¹ But Kouznetsov does not in any way teach obtaining application-specific intrusion criteria. In rejecting this claimed feature, the Office cites to, and underlines, a portion of Kouznetsov that does not describe application-specific intrusion criteria.²

¹ See Kouznetsov at Abstract.

² See Kouznetsov at col. 2, lines 51-58 and col. 5, lines 9-12 and col. 7, lines 1-2; and 12-10-2008 final Office Action at p. 2.

The sequence of the execution of the monitored events is tracked for each of the applications. Each occurrence of a specific event sequence characteristic of computer virus behavior and the application that performed the specific event sequence, are identified. A histogram describing the specific event sequence occurrence for each of the applications is created. Repetitions of the histogram associated with at least one object are identified.

However, a “specific event sequence characteristic of computer virus behavior”, as described in Kouznetsov, does not constitute intrusion criteria, but rather is the output of the tracking performed using intrusion criteria. Thus, the office has misconstrued the claimed subject matter when stating, “The underlined citation above reads on the claimed application-specific intrusion criteria that were tracked for each application as monitored events.”³ Attention is called to the fact that the present claims do not state that intrusion criteria are tracked. To the contrary, the present claims specify that network communications for the invoked application are monitored using the application-specific intrusion criteria.

In the Advisory Action, the Office states, “Examiner broadly and reasonable interprets intrusion criteria as something that is harming or causing unsafe, malware, intruders, or viruses.”⁴ Thus, the Office attempts to equate an intrusion into a computer system with intrusion criteria used to detect the intrusion. This claim construction defies common sense as it completely ignores the plain meaning of the word “criteria”. Moreover, this claim construction is also contradicted by the Office’s later statement that, “A (intrusive) criteria broadly and obviously can be any data/content that is considered to identify or measure what is deemed as intrusive or an intrusion.”⁵ Thus, the rejection of all the claims suffers from a clear legal or factual deficiency for at least this reason.

Far from teaching the use of application-specific intrusion criteria, Kouznetsov actually teaches the opposite. Kouznetsov teaches that the program state of the executing applications is monitored by a monitor/analyzer 19 that monitors all applications equally using apparently

³ See 12-10-2008 final Office Action at p. 2; emphasis added.

⁴ See 3-5-2009 Advisory Action at p. 2, 3rd ¶.

⁵ See 3-5-2009 Advisory Action at p. 2, 6th ¶.

common criteria.⁶ Nothing here, or in any other part of Kouznetsov, suggests that Kouznetsov's determination of whether the application is performing a sequence of suspicious actions characteristic of computer viruses is based on criteria specific to an application. Rather, Kouznetsov merely states that when a suspicious event sequence is identified, the application performing that event sequence is also identified. Thus, Kouznetsov does not in any way teach the claimed, "obtaining application-specific intrusion criteria" and "monitoring network communications for the invoked application [...] using the application-specific intrusion criteria to detect an intrusion."

The Office attempts to refute this argument by stating, "it is not as applicant stated as 'using' the application specific criteria but monitoring 'for' the invoked application as claimed."⁷ With all due respect to the Office, the basis for the Office's claim construction here cannot be understood. The claim language states, "monitoring network communications for the invoked application, after the examining and the obtaining, using the application-specific intrusion criteria to detect an intrusion." This clearly means that the network communications for the invoked application are monitored using the application-specific intrusion criteria to detect an intrusion, and any other claim construction would be legally invalid in light of the Specification. Thus, the rejection of all the claims suffers from a clear legal or factual deficiency for at least this additional reason.

Furthermore, neither Kouznetsov nor Gryaznov, either alone or in combination, teaches or suggests, "examining a set of instructions embodying an invoked application to identify the invoked application", as claimed.⁸ The cited portions of Kouznetsov teach traditional loading and executing of program code.⁹ Interpreting the present claim language, "examining a set of instructions embodying an invoked application" as reading on the traditional loading and executing of program code is inconsistent with the present specification and is thus an improper claim construction under the law and the MPEP.¹⁰ The Office has failed to address this point.

⁶ See Kouznetsov at col. 4, lines 15-27.

⁷ See 3-5-2009 Advisory Action at p. 2, 4th ¶.

⁸ Emphasis added.

⁹ See Kouznetsov at col. 2, lines 47-48 and col. 4, lines 12-14 and 28-47.

¹⁰ See e.g., MPEP § 2111.01.

Moreover, the Office's use of Gryaznov in combination with Kouznetsov to address the full claim feature, "examining a set of instructions embodying an invoked application to identify the invoked application", is without merit. The Office has split this claim feature into two parts: (1) "examining a set of instructions embodying an invoked application", and (2) "to identify the invoked application"; and the Office then attempts to combine Gryaznov with Kouznetsov to arrive at the full claim feature. Gryaznov describes a method, system, and computer program product that provides multiple names of a given malware in a quick and automated fashion.¹¹ As noted above, and in sharp contrast, Kouznetsov teaches a system and a method for dynamically detecting computer viruses through associative behavioral analysis of runtime state. The Office has provided no logical reasoning with some rational underpinning to combine these two references to support the legal conclusion of obviousness, as is required by law. The undersigned attorney has read the Response to Arguments section in the final Office Action on this point multiple times and fails to grasp the Office's position. In particular, the Office appears to confuse the claimed "examining a set of instructions embodying an invoked application to identify the invoked application" with the "obtaining application-specific intrusion criteria",¹² and the Office fails to "identify the reason why a person of ordinary skill in the art would have combined the prior art elements in the manner claimed."¹³ Further, the Advisory Action fails to clarify any logical reasoning underlying the proposed combination. Thus, the rejection of all the claims suffers from a clear legal or factual deficiency for at least this additional reason.

Moreover, claim 28 recites, "wherein examining the set of instructions comprises: applying a hash function to the set of instructions to generate a condensed representation; and comparing the condensed representation with existing condensed representations for known applications."¹⁴ The cited portion of Kouznetsov describes virus behavior in which a number of bytes are written into an application program file, but says nothing about applying a hash function to a set of instructions to generate a condensed representation.¹⁵ In fact, Kouznetsov

¹¹ See Gryaznov at Abstract.

¹² See 12-10-2008 final Office Action at pp. 2-3.

¹³ See Memorandum dated May 3, 2007, to Technology Center Directors from Margaret A. Focarino, Deputy Commissioner for Patent Operations, re Supreme Court decision on KSR Int'l. Co., v. Teleflex, Inc. (emphasis added).

¹⁴ Emphasis added.

¹⁵ See Kouznetsov at col. 5, lines 50-58.

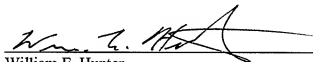
never even mentions the use of a hash function, let alone using a hash function to generate a condensed representation of a set of instructions and comparing the condensed representation with existing condensed representations for known applications. The Office has failed to address this point, either in the final Office action or in the Advisory Action, and the Office has provided no explanation of the basis for rejecting this claim. Thus, the rejection of claim 28 suffers from a clear legal or factual deficiency for at least this additional reason.

In view of the above, all of the claims should be in condition for allowance. A formal notice of allowance is thus respectfully requested.

Please apply the notice of appeal fee, and any other necessary charges or credits, to deposit account 06-1050.

Respectfully submitted,

Date: March 9, 2009


William E. Hunter
Reg. No. 47,671
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer No. 20985
Telephone: (858) 678-5070
Facsimile: (877) 769-7945